(51) Int. Cl. ²: G 07 C 9/00
B 44 F 1/12
G 06 K 19/00
G 07 D 7/00

(19) BUNDESREPUBLIK DEUTSCHLAND
DEUTSCHES PATENTAMT

DE 28 26 469 A 1

# (11) Offenlegungsschrift 28 26 469

(21) Aktenzeichen: P 28 26 469.9-53
(22) Anmeldetag: 16. 6. 78
(43) Offenlegungstag: 20. 12. 79

(30) Unionspriorität:
(32) (33) (31) —

(54) Bezeichnung: Verfahren und Einrichtung zur Absicherung von Dokumenten

(71) Anmelder: Scheffel, Kurt, 7858 Weil

(72) Erfinder: Nichtnennung beantragt

Prüfungsantrag gem. § 28 b PatG ist gestellt

DE 28 26 469 A 1

● 12. 79 909 851/443 20/80

PATENTANWALT DIPL.-ING. GERHARD SCHWAN
ELFENSTRASSE 32 · D-8000 MÜNCHEN 83

2826469

## Ansprüche

1. Verfahren zur Erzeugung und Kontrolle von gegen Nachahmung, Verfälschung und Mißbrauch abgesicherten Dokumenten, bei dem auf dem abzusichernden Dokument eine Information maschinell lesbar in unverschlüsselter und in verschlüsselter Form eingetragen und zur Kontrolle die verschlüsselte Information entschlüsselt und mit der unverschlüsselten Information verglichen wird, dadurch gekennzeichnet, daß zur Verschlüsselung der auf dem Dokument verschlüsselt eingetragenen Information ein Algorithmus bzw. ein diesem zugeordneter Schlüssel verwendet wird, der gegen Ableitung aus dem bei der Kontrolle des Dokumentes zur Entschlüsselung verwendeten Algorithmus bzw. dessen Schlüssel gesichert ist.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zur Erzeugung des abgesicherten Dokuments eine im voraus auf das noch ungesicherte Dokument unverschlüsselt aufgebrachte Information automatisch ausgelesen, verschlüsselt und zusammen mit dem Schlüssel des bei der Kontrolle des Dokuments zu verwendenden Algorithmus auf dem Dokument eingetragen wird.

909851/0443
FERNSPRECHER: 089/6012039 · KABEL: ELECTRICPATENT MÜNCHEN
ORIGINAL INSPECTED

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß für jedes Dokument in Abhängigkeit von einer Zufallszahl ein Paar von Schlüsseln erzeugt wird, von denen der eine zum Verschlüsseln der unverschlüsselt aufgezeichneten Information und der andere zum Entschlüsseln der verschlüsselt aufgezeichneten Information verwendet wird.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß eine vorbestimmte Folge von Schlüsselpaaren vorgesehen wird, für die Erzeugung des abgesicherten Dokuments eine im voraus auf das noch ungesicherte Dokument unverschlüsselt aufgebrachte Information automatisch ausgelesen und zum Eintragen auf das Dokument unter Verwendung des einen der beiden Schlüssel eines Schlüsselpaares verschlüsselt wird, das aus der Folge in Abhängigkeit von der unverschlüsselten Information selbsttätig ausgewählt wird, sowie daß bei der Kontrolle aus der Folge der zur Entschlüsselung zu verwendenden Schlüssel anhand der unverschlüsselten Information der zugehörige Schlüssel selbsttätig ausgewählt und mit ihm die verschlüsselt eingetragene Information entschlüsselt wird.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zur Erzeugung des abgesicherten Dokuments eine im voraus auf das noch ungesicherte Dokument unverschlüs-

selt aufgebrachte Information automatisch ausgelesen, entsprechend einem fest vorgegebenen Schlüssel verschlüsselt und auf dem Dokument eingetragen wird, sowie daß bei der Kontrolle der gleichfalls fest vorgegebene zugehörige Schlüssel für das Entschlüsseln der verschlüsselt aufgebrachten Information verwendet wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß in die Verschlüsselung zur Personalisierung des Dokuments eingetragene Informationen einbezogen werden.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß bei der Dokumentenerzeugung eine Identifikationsnummer auf dem Dokument verschlüsselt aufgezeichnet sowie bei der Kontrolle die aus dem Dokument selbsttätig ausgelesene und entschlüsselte Identifikationsnummer mit einer vom Benutzer des Dokuments unverschlüsselt einzugebenden Identifikationsnummer verglichen wird.

8. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß bei der Dokumentenerzeugung ein vom Benutzer des Dokuments gesprochenes Codewort oder dergleichen in eine digitale Form umgewandelt und auf dem Dokument verschlüsselt aufgezeichnet wird, sowie daß bei der Kontrolle die aus dem Do-

kument selbsttätig ausgelesenen und entschlüsselten Codewortsignale mit Signalen verglichen werden, die durch Digitalisieren des vom Benutzer des Dokuments zu Kontrollzwecken gesprochenen Codeworts gewonnen werden.

9. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß bei der Dokumentenerzeugung aus einer auf das Dokument aufgebrachten, den Benutzer identifizierenden bildlichen Darstellung digitale Signale abgeleitet und auf dem Dokument verschlüsselt aufgezeichnet werden, und daß bei der Kontrolle diese Bildsignale aus dem Dokument selbsttätig ausgelesen und entschlüsselt sowie mit Bildsignalen verglichen werden, die für die Kontrolle aus der bildlichen Darstellung selbst abgeleitet werden.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, daß die bildliche Darstellung innerhalb eines gedachten Rasterfeldes abgetastet wird, das mit der bildlichen Darstellung eine Ecke und zwei Kanten gemeinsam hat, und daß die Helligkeitswerte der einzelnen Rasterpunkte so gewichtet werden, daß ein vorgeschriebenes Verhältnis der Anzahlen von als hell bzw. als dunkel gewerteten Rasterpunkten entsteht.

11. Einrichtung zur Erzeugung von abgesicherten Dokumenten gemäß dem Verfahren nach einem der vorhergehenden Ansprüche, gekennzeichnet durch einen Geber (3, 4) für mindestens ein Paar von Schlüsselzahlen nach einer trap-door-Funktion, einen Dokumentenleser (6) zum automatischen Lesen von Informationen auf dem Dokument, einen Algorithmusrechner (5) zur Verschlüsselung der auf dem Dokument gelesenen Information mit der geheimgehaltenen Schlüsselzahl und einen Dokumentenschreiber (7) zum Eintragen der für die Entschlüsselung notwendigen Schlüsselzahl und der verschlüsselten Information auf dem Dokument.

12. Einrichtung zur Kontrolle von abgesicherten Dokumenten gemäß dem Verfahren nach einem der Ansprüche 1 bis 10, gekennzeichnet durch einen Dokumentenleser (15) zum automatischen Lesen der unverschlüsselten Information einen Dokumentenleser (16) zum automatischen Lesen der zur Entschlüsselung notwendigen Schlüsselzahl und der verschlüsselten Information, einen Algorithmusrechner (12) zur Entschlüsselung der verschlüsselten Information unter Verwendung der gelesenen Schlüsselzahl und einen Vergleicher (13) für die unverschlüsselte und die entschlüsselte Information.

13. Einrichtung nach Anspruch 11, dadurch gekennzeichnet, daß der Schlüsselzahlgeber (3, 4) einen Schlüsselgenerator (4) zur Erzeugung von Paaren von Schlüsselzahlen aufweist.

14. Einrichtung nach Anspruch 13, dadurch gekennzeichnet, daß dem Schlüsselgenerator (4) ein Zufallszahlen liefernder Zufallsgenerator (3) vorgeschaltet ist.

15. Einrichtung nach einem der Ansprüche 11, 13 oder 14, gekennzeichnet durch einen Datenträgerleser (21) für Personalisierungsdaten und ein Schreibgerät (22), mittels dessen die aus den Personalisierungsdaten abgeleiteten unverschlüsselten und verschlüsselten Informationen auf einem Leerformular eintragbar sind.

16. Einrichtung nach einem der Ansprüche 11 oder 13 bis 15, gekennzeichnet durch einen Generator (25) für persönliche Identifikationsnummern, der an den Algorithmusrechner (5) zwecks Verschlüsselung der erzeugten persönlichen Identifikationsnummer zur Eintragung auf dem Dokument angeschlossen ist.

17. Einrichtung nach einem der Ansprüche 11 oder 13 bis 16, gekennzeichnet durch ein Sprachverschlüsselungsgerät (50) zur Digitalisierung eines auf einem Datenträger

enthaltenen gesprochenen Textes, der über den Algorithmusrechner (5) in verschlüsselter Form auf dem Dokument eintragbar ist.

18. Einrichtung nach einem der Ansprüche 11 oder 13 bis 17, gekennzeichnet durch ein dem Algorithmusrechner (5) vorgeschaltetes Bildrasterabtastgerät (33) zur Digitalisierung eines auf dem Dokument angebrachten Bildes.

19. Einrichtung nach Anspruch 12, gekennzeichnet durch eine dem Vergleicher (13) vorgeschaltete Eingabevorrichtung (28) zur Eingabe einer persönlichen Identifikationsnummer.

20. Einrichtung nach Anspruch 12 oder 19, gekennzeichnet durch ein Mikrofon (51) und ein dem Mikrofon nachgeschaltetes, mit einem Eingang des Vergleichers (13) verbundenes Sprachverschlüsselungsgerät (50) zur Digitalisierung der mittels des Mikrofons aufgenommenen Sprachsignale.

21. Einrichtung nach Anspruch 12, dadurch gekennzeichnet, daß dem Vergleicher (13) ein Bildrasterabtastgerät zur Digitalisierung eines auf dem Dokument vorgesehenen Bildes vorgeschaltet ist.

2826469

Ing. Kurt Scheffel, Breslauer Str. 1,
7858 Weil am Rhein

# Verfahren und Einrichtung zur Absicherung von Dokumenten

Die Erfindung betrifft ein Verfahren und eine Einrichtung zur Erzeugung und Kontrolle von gegen Nachahmung, Verfälschung und Mißbrauch abgesicherten Dokumenten, insbesondere Ausweiskarten.

In zunehmendem Maße wird es erforderlich, Ausweiskarten, Paßkarten, Führerscheine oder ähnliche Dokumente statt wie bisher nur visuell nunmehr auch automatisch zu kontrollieren, insbesondere um die Abfertigung an Massenverkehrspunkten, wie Flughäfen und Grenzübergängen, zu beschleunigen, aber auch um die in den Ausweisen enthaltenen Informationen automatisch an eine Stelle übermitteln zu können, wo sie mit entsprechenden Listen verglichen werden können.

Darüberhinaus erscheint es nützlich, die Echtheit oder Unversehrtheit eines Ausweises, die bisher ausschließlich durch den Menschen geprüft werden, durch eine automatische Prüfung zu unterstützen.

Der durch automatisch arbeitende Verfahren und Geräte durchgeführten Absicherung solcher Ausweisdokumente kommen verschiedene Aufgaben zu. Besonders wichtig ist die Absicherung gegen von Fälschern hergestellte Dokumente. Bei dem heutigen Stand der Fälschungstechnik erscheint eine maschinelle Kontrolle des Dokumentes auf Echtheit unerläßlich, zumal die visuelle Kontrolle auch darunter leidet, daß die Schulung der Kontrollbeamten immer schwieriger wird. Unbedingt erforderlich wird eine automatische Echtheitskontrolle dann, wenn, wie z.B. in Ballungszentren des Reiseverkehrs, auf eine visuelle Kontrolle ganz verzichtet werden muß, um die Abfertigung zu beschleunigen.

Eine weitere Aufgabe der automatischen Absicherung von Dokumenten besteht im Schutz der aus den Dokumenten visuell oder automatisch herauslesbaren Information. Für die Automatisierung dieser Kontrolle gelten die gleichen Gründe wie die oben genannten. Bei der Unterstützung der visuellen Kontrolle durch eine automatische Kontrolle sollten zu den schutzbedürftigen Informationen zweck-

mäßig auch bildliche Darstellungen, wie z.B. das Foto des Ausweisinhabers, zählen.

Ferner soll verhindert werden, daß mit gestohlenen, noch nicht personalisierten Ausweisdokumenten Mißbrauch getrieben werden kann, wie es z.B. mit gestohlenen Paßformularen heute geschieht, indem diese nachträglich durch den Fälscher mit allen Personalisierungsdaten wie auch einem Foto versehen werden.

Eine weitere wichtige Aufgabe der automatischen Kontrolle besteht in der Sicherung gegen Verlust durch den rechtmäßigen Inhaber. Ein echtes personalisiertes Ausweisdokument soll nur vom rechtmäßigen Inhaber benutzt werden können. Hierzu zählen vor allen Dingen Ausweisdokumente, die kein Foto tragen oder keiner visuellen Kontrolle unterliegen.

Im Gegensatz zu z.B. Banknoten oder Wertpapieren ist ein Schutz gegen Duplizierung durch den Fälscher nicht erforderlich. Die Herstellung eines Duplikates eines personalisierten Ausweispapieres ist keine Aufgabe, die sich dem Fälscher stellt.

Zur Lösung der oben genannten Probleme sind eine Vielzahl von Methoden genannt worden, die im allgemeinen aber nicht

allen angeführten Aufgaben gerecht werden können und außerdem Nachteile haben, die die Handhabung erschweren oder die Absicherung unvollkommen machen.

Es ist bekannt, Ausweisdokumente mit einer maschinell lesbaren Schrift, z.B. einer OCR-Schrift, die optisch gelesen werden kann, einer MCR-Schrift, die magnetisch und visuell gelesen werden kann, einer optisch oder magnetisch automatisch lesbaren Balkenschrift oder einem entsprechend codierten Magnetstreifen zu versehen. Es ist auch bekannt, solche maschinell lesbaren Zeichen zur Eintragung verschlüsselter Informationen zu verwenden, die mit anderen Informationen des Ausweisdokumentes über einen Algorithmus zusammenhängen. Eine derartige Verschlüsselung bietet für die Herstellung von falschen Ausweisdokumenten kein wesentliches Hindernis. Die Einrichtungen, mit denen die verschlüsselte Information mit der unverschlüsselten Information verglichen wird, um die Echtheit und die Unversehrtheit der Ausweisdokumente zu prüfen, müssen an vielen Stellen, z.B. bei Polizeistationen oder Grenzübergängen vorhanden sein und sind daher einem räuberischen Zugriff offen. Aus diesen Einrichtungen läßt sich der verwendete Algorithmus ableiten, auch wenn er vorher geheimgehalten wurde.

Darüberhinaus ist es mit modernen Methoden der Dechiffrier-

technik möglich, den Algorithmus aus einer größeren Anzahl von Ausweisdokumenten verschiedenen Inhaltes zu ermitteln.

Weiterhin ist vorgeschlagen worden, Ausweisdokumente so zu gestalten, daß eine Änderung der auf ihnen eingetragenen Information als ganze oder teilweise Zerstörung des Dokumentes sichtbar wird. Die bisher bekannten Verfahren scheinen zwar im visuellen Bereich brauchbar zu sein, die meisten von ihnen scheiden aber für eine automatische Kontrolle aus.

Als zur Zeit beste Möglichkeit, eine Absicherung gegen Verlust oder Diebstahl des Ausweisdokumentes vorzunehmen, gilt die persönliche Identifikationsnummer, abgekürzt "PIN". Die PIN ist eine Zahl oder ein anderer Merkbegriff, die nur dem rechtmäßigen Inhaber des Ausweisdokumentes bekannt sein soll und die er während der automatischen Kontrolle des Ausweisdokumentes in eine Tastatur oder dergleichen eingibt. Die PIN ist im Ausweisdokument über einen Algorithmus verschlüsselt maschinell lesbar enthalten, so daß die Kontrolleinrichtung einen Vergleich der beiden Eingaben durchführen kann. Auch die PIN bietet aber keinen eindeutigen Schutz, da der Algorithmus zu ihrer Verschlüsselung und damit die PIN selbst dem Fälscher auf einem der oben genannten Wege bekannt werden kann.

Man hat ferner vorgeschlagen, für den Aufbau von Ausweisdokumenten Materialien zu verwenden, die dem Fälscher nicht zugänglich sind wie z.B. radioaktive Materialien, die einer staatlichen Kontrolle unterliegen, und diese Materialien in einer entsprechenden Kontrollapparatur feststellen zu lassen. Wenn es wirklich gelingt, diese Materialien unter Kontrolle zu halten oder geheimzuhalten, so ist damit ein Schutz gegen die Nachahmung von Ausweisdokumenten möglich. Ein Schutz gegen die Veränderung der auf den Ausweisdokumenten enthaltenen Information ergibt sich durch diese Methode jedoch nicht. Außerdem erscheint die Monopolisierung der Herstellung und Verwendung solcher Materialien schwierig, da bei ihrer Herstellung und Verwendung zwangsweise eine größere Anzahl von Personen beschäftigt sein muß und dadurch ein Diebstahl solcher Materialien nicht zu verhindern ist bzw. bei geheimzuhaltenden Materialien der Verrat der Geheimnisse nicht auszuschließen ist.

Die im folgenden beschriebene Erfindung setzt es sich zum Ziel, die genannten Mängel der bekannten Methoden zu vermeiden und darüberhinaus ein einfach anzuwendendes wirtschaftliches Verfahren mit nicht aufwendigen Geräten zu schaffen, das allen oben genannten Kriterien gleichermaßen gerecht wird.

Ausgehend von einem Verfahren zur Erzeugung und Kontrolle von gegen Nachahmung, Verfälschung und Mißbrauch abgesicherten Dokumenten, bei dem auf dem abzusichernden Dokument eine Information maschinell lesbar in unverschlüsselter und in verschlüsselter Form eingetragen und zur Kontrolle die verschlüsselte Information entschlüsselt und mit der unverschlüsselten Information verglichen wird, wird diese Aufgabe erfindungsgemäß dadurch gelöst, daß zur Verschlüsselung der auf dem Dokument verschlüsselt eingetragenen Information ein Algorithmus bzw. ein diesem zugeordneter Schlüssel verwendet wird, der gegen Ableitung aus dem bei der Kontrolle des Dokumentes zur Entschlüsselung verwendeten Algorithmus bzw. dessen Schlüssel gesichert ist. Das heißt, für die Verschlüsselung wird ein geheimgehaltener Algorithmus verwendet, der auf einer trap-door-Funktion beruht und daher nicht aus dem zum Entschlüsseln verwendeten, nicht notwendig geheimgehaltenen Algorithmus abgeleitet werden kann.

In weiterer Ausgestaltung der Erfindung werden in die auf dem Dokument enthaltenen, zu verschlüsselnden Informationen auch bildliche Darstellungen mit einbezogen.

Nach einem weiteren wesentlichen Erfindungsgedanken werden in die Verschlüsselung auch Kennzeichen des rechtmäßigen Inhabers, wie z.B. eine persönliche Identifikationsnummer,

ein Foto, eine Unterschrift oder ein gesprochenes Losungswort einschließlich den klanglichen Merkmalen der Stimme des rechtmäßigen Inhabers, aufgenommen.

Weitere Merkmale der Erfindung ergeben sich aus den Unteransprüchen. Die Erfindung ist im folgenden anhand von bevorzugten Ausführungsbeispielen in Verbindung mit den Zeichnungen näher erläutert. Es zeigen:

Fig. 1 eine Einrichtung zur Absicherung von Dokumenten,

Fig. 2 eine Einrichtung zur Kontrolle abgesicherter Dokumente,

Fig. 3 eine Einrichtung zur Personalisierung und Absicherung von Dokumenten unter Einbeziehung einer persönlichen Identifikationsnummer,

Fig. 4 eine Einrichtung zur Kontrolle von abgesicherten Dokumenten mit persönlicher Identifikationsnummer,

Fig. 5 eine Einrichtung zur Personalisierung und Absicherung von Dokumenten

unter Einbeziehung der Codewort- und Klangerkennung,

Fig. 6 eine Einrichtung zur Kontrolle abgesicherter Dokumente unter Einbeziehung der Codewort- und Klangerkennung,

Fig. 7 einen Abtastraster für eine bildliche Darstellung und

Fig. 8 eine Schaltungsanordnung zur Erzeugung eines vorgegebenen Verhältnisses der Anzahlen von hellen und dunklen Rasterpunkten.

Jede Chiffrierung beruht darauf, die zu chiffrierende Information K durch Anwendung eines Algorithmus A in die chiffrierte Information C zu verwandeln.

$$C = A(K) \qquad (1)$$

Nach Übermittlung der chiffrierten Information C dechiffriert der Empfänger diese chiffrierte Information durch Anwendung eines Algorithmus B und erhält die

dechiffrierte Information K.

$$K = B(C) \qquad (2)$$

Die Algorithmen A und B beinhalten in modernen Chiffrierverfahren meist zwei Bestandteile, nämlich ein Rechenverfahren und eine Schlüsselinformation. So besteht z.B. ein bekanntes Verfahren zur Verschlüsselung und Entschlüsselung von Informationen auf Fernschreibleitungen darin, daß auf der Sendeseite zu der zu verschlüsselnden Information Bit für Bit stochastische Information addiert und die gleiche Information auf der Empfangsseite wieder Bit für Bit subtrahiert wird. Hier erhält der Algorithmus A das Additionsverfahren, der Algorithmus B das Subtraktionsverfahren, und die Schlüsselinformation besteht in der an beiden Stellen gleichen stochastischen Bitfolge.

Wie in diesem Fall, so ist es in den meisten Chiffrier- und Dechiffrierverfahren möglich, die in den Algorithmen enthaltenen Rechenverfahren bekanntzugeben und zur Sicherung der übertragenen chiffrierten Nachrichten nur die Schlüsselinformation geheimzuhalten.

Alle bis vor wenigen Jahren angewendeten Verschlüsselungsverfahren haben aber die Eigenschaft, daß die Algorithmen A und B bzw. bei nicht geheimgehaltenen Rechenverfahren die

zu A und B gehörenden Schlüsselinformationen auseinander ableitbar sind. In dem oben beschriebenen Fall der Fernschreibverschlüsselung müssen die Schlüsselinformationen sogar exakt gleich sein.

In Verbindung mit dem Transport von geheimzuhaltenden Nachrichten über Leitungen sind in den letzten Jahren Algorithmen bekannt geworden, für die das nicht mehr zutrifft. Obwohl diese Algorithmen die in den Gleichungen (1) und (2) dargestellte Eigenschaft, nämlich bei aufeinanderfolgender Anwendung die ursprüngliche Information wiederherzustellen, besitzen, ist es doch unmöglich, aus dem Algorithmus A den Algorithmus B abzuleiten, selbst dann nicht, wenn außer dem Algorithmus A eine größere Zahl von unverschlüsselten Informationen K und zugehörigen, verschlüsselten Informationen C gegeben sind. Derartige Algorithmen werden in der amerikanischen Literatur "trap-door"-Funktionen genannt.

Auch für die Verschlüsselung auf der Basis der trap-door-Funktionen gilt die Möglichkeit der Zerlegung in die beiden Bestandteile: Rechenverfahren und Schlüsselinformation. Auch bei ihnen kann das Rechenverfahren bekanntgemacht werden. Die trap-door-Eigenschaft bleibt auch dann erhalten, wenn nur die Schlüsselinformation des Algorithmus B geheimgehalten wird.

Das Verfahren und die Einrichtung nach der Erfindung nutzen die Eigenschaften der trap-door-Funktionen für den Schutz von Dokumenten.

Fig. 1 zeigt ein Gerät wie es z.B. in einer Paßbehörde zur Absicherung von Paßkarten verwendet werden kann. Es wird zur Erhöhung der Anschaulichkeit in einem Teil der Beschreibung von "Karten" gesprochen. Alle beschriebenen Verfahren und Einrichtungen lassen sich aber auf andere Dokumente übertragen. Ein Codierrechner 1 ist mit einem Kartenleser-/schreiber 2 verbunden. Der Codierrechner 1 enthält einen Zufallsgenerator 3, einen Schlüsselgenerator 4 und einen Algorithmusrechner 5.

Der Kartenleser/-schreiber besteht aus einem Kartenleser 6, der von der ungesicherten Karte eine Information liest und einem Kartenschreiber 7, der auf die Karte die zur Absicherung dienende Information aufschreibt.

Die beschriebene Einrichtung arbeitet folgendermaßen: Bei der Einführung einer Karte in den Kartenleser 6 wird der Zufallsgenerator 3 in Betrieb gesetzt; er liefert eine Zufallszahl X. Diese Zufallszahl wird im Schlüsselgenerator 4 in zwei Schlüsselzahlen A und B umgerechnet. Der Schlüsselgenerator 4 ist in seinem Aufbau und/oder seiner Programmierung für die Herstellung von Schlüsselzahlen

eingerichtet, die die trap-door-Eigenschaft besitzen. Das bedeutet, daß die Schlüsselzahl B sich nicht mit vertretbarem Aufwand aus der Schlüsselzahl A errechnen läßt.

Solche Rechenverfahren sind an sich bekannt und in der Literatur beschrieben. Der Aufbau und/oder die Programmierung eines Rechners, der als Schlüsselgenerator 4 verwendet werden kann, sind daher für den Fachmann möglich.

Die von der ungesicherten Karte über den Kartenleser 6 abgelesene Information K wird dem Algorithmusrechner 5 zugeführt, der mit einem nicht notwendig geheim gehaltenen Rechenverfahren aber mit der geheim gehaltenen Schlüsselzahl B hieraus die verschlüsselte Information C nach folgender Gleichung herstellt:

$$C = B\ (K) \qquad (3)$$

Dieser verschlüsselten Information wird die vom Schlüsselgenerator 4 erzeugte Schlüsselzahl A vorangestellt; beide Informationen werden mit Hilfe des Kartenschreibers 7 auf die Karte geschrieben.

Die Einrahmung der zum Codierrechner 1 gehörenden Einrichtungsteile soll andeuten, daß diese Geräte vor Zugriff gesichert sind.

Die Einrahmung der zum Kartenleser/-schreiber 2 gehörenden

Einrichtungsteile soll dagegen andeuten, daß Kartenleser 6 und Kartenschreiber 7 mechanisch oder auf andere Weise so miteinander verbunden sind, daß die vom Codierrechner 1 erzeugte Information mittels des Kartenschreibers 7 auf die gleiche Karte geschrieben wird, von der die unverschlüsselte Information mittels des Kartenlesers 6 gelesen wurde.

Fig. 2 stellt in beispielhafter Ausführung das Prüfgerät für abgesicherte Ausweiskarten dar. In diesem Prüfgerät sind keinerlei geheime Elemente enthalten, so daß es gegen einen Zugriff nicht geschützt werden muß. Der Prüfrechner 11 besteht aus einem Algorithmusrechner 12 und einem Vergleicher 13, der als Ausgang eine Ja/Nein-Aussage 17 liefert. Zum Prüfrechner 11 gehört ein Kartenlesegerät 14, das Kartenleser 15 und 16 aufweist. Mit dem Kartenleser 15 wird die gleiche Information K gelesen wie vom Kartenleser 6 aus Fig. 1, während der Kartenleser 16 die Information liest, die der Kartenschreiber 7 auf der Karte eingetragen hat. Sind diese beiden Informationen in der gleichen physikalischen Weise und an einander zugeordneten geometrischen Stellen der Karte realisiert, können die Kartenleser 15 und 16 auch zu einem gemeinsamen Leser verschmolzen werden.

Die beschriebene Einrichtung arbeitet folgendermaßen:

Die Karte wird in das Lesegerät 14 eingeführt. Es werden nacheinander die unverschlüsselte Information K und danach die vom Codierrechner 1 erzeugte Information gelesen. Die letztgenannte Information durchläuft den Algorithmusrechner 12.

Hierbei wird zunächst vom Leser 16 der vom Kartenschreiber 7 in die Karte eingetragene Schlüssel A gelesen. Diesen Schlüssel A verwendet der Algorithmusrechner 12 bei der Entschlüsselung der vom Kartenschreiber 7 eingetragenen verschlüsselten Information C. Das Ergebnis ist die unverschlüsselte Information K nach folgender Gleichung:

$$K = A\ (C) \qquad (4)$$

die mit der direkt gelesenen unverschlüsselten Information K im Vergleicher 13 verglichen wird. Der Vergleicher 13 gibt bei Übereinstimmung der beiden Informationen ein Ja-, bei Nicht-Übereinstimmung ein Nein-Signal 17 ab.

Man kann in der Dokumentensicherungs-Einrichtung nach Fig. 1 Leerdokumente verwenden, die nicht personalisiert sind, also noch keine Daten des zukünftigen Inhabers tragen, dagegen aber, wie es z. B. bei Reisepässen üblich ist, laufend numeriert sind. Derartige Dokumente sind insoweit gegen Fälschung geschützt, als es dem Fälscher nur möglich ist, von einem ihm zur Verfügung stehenden Leerdokument exakte Duplicate herzustellen. Er ist aber ohne den Schlüssel B nicht in der Lage, Fälschungen mit abweichenden Paß-

nummern anzufertigen.

Zugleich ist bei den echten Dokumenten die laufende Numerierung gegen Abänderung geschützt. Jede Abänderung der unverschlüsselten Paßnummer wie auch der verschlüsselten Paßnummer wird von der Dokumentenprüfeinrichtung nach Fig. 2 erkannt.

Führt man der Dokumentensicherungs-Einrichtung nach Fig. 1 dagegen personalisierte Ausweise zu, also solche, die Informationen über den rechtmäßigen Inhaber enthalten, so werden diese Informationen ebenfalls dem Verschlüsselungsverfahren unterworfen.

Sie können hierzu in einer zugleich visuell und automatisch lesbaren Schrift wie OCR oder MICR eingetragen sein. Es können auch neben der visuell lesbaren Schrift dieselben Informationen in codierter Form eingetragen sein, z.B. auf dem Magnetstreifen eines Ausweises. Schließlich können die zu schützenden Informationen in einer bildlichen Darstellung oder einem Foto bestehen, wozu zweckmäßigerweise ein weiter unten beschriebenes Verfahren verwendet wird.

Die verschlüsselte Information einschließlich des Schlüssels A wird von dem Kartenschreiber 7 auf dem gleichen Dokument entweder nach dem gleichen oder einem abweichenden physika-

lischen Verfahren wie die unverschlüsselte Information dargestellt. Besonders einfache Geräte ergeben sich, wenn die unverschlüsselte Information und die verschlüsselte Information beide auf Magnetstreifen des Dokumentes, evtl. sogar in der gleichen Spur, eingetragen werden. Das ist natürlich nicht möglich, wenn zur unverschlüsselten Information etwa die Unterschrift oder das Foto des rechtmäßigen Karteninhabers gehören.

Bei der Prüfung abgesicherter, personalisierter Ausweise arbeitet die Dokumenten-Prüfeinrichtung nach Fig. 2 genauso, wie zuvor beschrieben. Ein Ja-Signal der Dokumenten-Prüfeinrichtung nach Fig. 2 ergibt sich nur dann, wenn weder die unverschlüsselte noch die verschlüsselte Information geändert wurden.

Bisher wurde vorausgesetzt, daß der vom Schlüsselgenerator 4 erzeugte Schlüssel A in Klartext auf dem Dokument eingetragen wurde und bei der Prüfung in der Dokumenten-Prüfeinrichtung nach Fig. 2 abgelesen und im Algorithmusrechner 12 verwendet wurde.

Zur Vereinfachung des Verfahrens ist es möglich, für eine bestimmte Klasse von Ausweisen, z.B. für die Paßkarten eines Landes, die Herstellung der Schlüssel A und B nur einmal vorzunehmen und den Schlüssel A unveränderlich in allen

Dokumentations-Prüfeinrichtungen nach Fig. 2 einzubauen. In diesem Falle kann der Zufallsgenerator 3 entfallen; die nur einmal benötigte Zufallszahl X kann auf andere Weise hergestellt werden.

Zwischen den beiden Extremen, nur ein Paar von Schlüsseln A und B zu verwenden bzw. für jede Karte ein neues Paar von Schlüsseln A und B zu generieren, liegt die Verfahrensvariante, eine begrenzte Anzahl von solchen Schlüsselpaaren herzustellen und als Liste im Codierrechner 1 aufzubewahren. In diesem Falle wird im Codierrechner 1 sowohl auf den Zufallsgenerator als auch auf den Schlüsselgenerator verzichtet. Es muß nur dafür gesorgt werden, daß bei der Erzeugung der Schlüsselpaare A und B und bei ihrer Einbringung in den gegen Zugriff geschützten Codierrechner 1 die Geheimhaltung gewahrt wird. Mit bekannten Mitteln ist es möglich, eine begrenzte Anzahl solcher Schlüsselpaare in einem Speicher des Codierrechners 1 zu speichern, ohne daß sie den dabei beschäftigten Personen angezeigt oder gar ausgedruckt werden.

Das für eine Absicherung notwendige Schlüsselpaar muß aufgrund der mit dem Kartenleser 6 vom Dokument abgelesenen unverschlüsselten Information mit seiner Listen-Nummer abgerufen werden. Brauchbare Teile der unverschlüsselten Information zur Bildung der Listen-Nummer sind z.B. die Paß-

nummer, das Geburtsdatum, bestimmte Buchstaben des Namens usw.

In der Dokumenten-Prüfeinrichtung nach Fig. 2 ist für diese Variante eine entsprechende Liste der Schlüssel A vorhanden, die mit den gleichen Nummern versehen ist wie die Liste der Schlüsselpaare in der Dokumentensicherungs-Einrichtung nach Fig. 1. Auch hier wird die Listen-Nummer des richtigen Schlüssels A aus der Information abgeleitet, die der Leser 15 als unverschlüsselte Information auf dem Dokument findet.

Dokumente, die in der beschriebenen Weise gesichert werden, sind zusätzlich zu dem oben beschriebenen Schutz auch gegen jede Verfälschung der zur Personalisierung eingetragenen Information gesichert. Es ist mit der Dokumenten-Prüfeinrichtung nach Fig. 2 möglich, festzustellen, ob die für die visuelle Kontrolle dienende Information abgeändert wurde, insoweit diese Information in die abzusichernde Information mit einbezogen wurde.

Enthält das Dokument die den rechtmäßigen Inhaber betreffende Information in unverschlüsselter und in verschlüsselter Form auf einem Magnetstreifen, so kann die unverschlüsselte Form nach Kontrolle durch die Dokumenten-Prüfeinrichtung nach Fig. 2 getrennt abgespeichert

und später z. B. in einem Zentral-Rechner der Behörde verarbeitet werden.

In Fig. 3 ist eine Dokumentensicherungs-Einrichtung schematisch dargestellt, mit der Leerdokumente nicht nur gesichert, sondern auch automatisch personalisiert werden. Außerdem soll anhand der Fig. 3 die Möglichkeit, das Dokument gegen Verlust zu sichern, beschrieben werden. Diese letztere Möglichkeit läßt sich ohne weiteres auch auf die Dokumentensicherungs-Einrichtung nach Fig. 1 übertragen. Als praktische Anwendung wird wiederum die Herstellung von Paßkarten angenommen.

Der Codierrechner 27 ist ähnlich aufgebaut wie der Codierrechner nach Fig. 1. Zur Einspeisung der zu verschlüsselnden Daten dient in diesem Fall aber ein Datenträgerleser, vorzugsweise in Form eines Bandgerätes 21, in das die z.B. dezentral vorbereiteten Bänder mit den Personalisierungsdaten der zukünftigen Paßinhaber eingelegt werden. Die gleichen Daten werden einem Schreibgerät 22 zugeführt, das mit seiner Schreibeinheit 23 auf Leerformulare die Personalisierungsdaten in Klarschrift, z.B. visuell und maschinell lesbar, einträgt. Zugleich werden die vom Codierrechner abgegebenen Daten über eine weitere Schreibeinheit 24 des Bandgerätes 22 auf dem gleichen Dokument in maschinell lesbarer Schrift eingetragen.

Der Codierrechner 27 enthält außer den genannten Geräten noch einen Generator für die persönliche Identifikationsnummer (PIN). Diesem PIN-Generator 25 wird die vom Zufallsgenerator 3 erzeugte Zufallszahl X ebenfalls zugeführt, die er in eine z. B. vierstellige PIN verwandelt. Diese vierstellige PIN wird im Algorithmusrechner 5 zusätzlich zu der mittels des Bandgerätes 21 vom Magnetband abgelesenen unverschlüsselten Information eingespeist, verschlüsselt und von der Schreibeinheit 24 zusätzlich auf dem Dokument niedergeschrieben.

Gleichzeitig wird die PIN über einen Drucker 26 z.B. auf einen Versand- oder Ausgabeumschlag gedruckt, in dem die mit dem Schreibgerät 22 personalisierte Karte automatisch und synchron eingelegt wird. Es ist auch möglich, den späteren Benutzer der Karte die PIN selbst auswählen zu lassen und sie in das vom Bandgerät 21 zu lesende Magnetband mit aufzunehmen. In diesem Fall entfällt in der Einrichtung nach Fig. 3 der PIN-Generator 25.

Zur besseren Geheimhaltung ist es auch möglich, mit dem Drucker 26 einen Begleitzettel herzustellen, auf dem die PIN vermerkt ist. Der Begleitzettel wird seinerseits in einen mit einem nicht eingezeichneten Drucker nach den Angaben des Bandgerätes 21 beschrifteten adressierten Umschlag eingelegt und dem zukünftigen Inhaber des Dokumen-

tes unabhängig vom Dokument zugestellt.

Fig. 4 zeigt die entsprechend erweiterte Dokumenten-Prüfeinrichtung. Sie enthält außer den bereits in Fig. 2 dargestellten Teilen noch ein Eingabegerät 28, vorzugsweise in Form einer Tastatur, in die der Inhaber des Dokumentes aus dem Gedächtnis seine PIN eintastet. Der Vergleicher 13 übernimmt zusätzlich zu den bereits beschriebenen Aufgaben den Vergleich der eingetasteten PIN mit der über den Algorithmusrechner 12 entschlüsselten PIN und gibt sein Ja-Signal nur dann ab, wenn beide Vergleiche stimmen.

In neuerer Zeit sind Einrichtungen bekannt geworden, mit denen bestimmte Worte, von verschiedenen Menschen ausgesprochen, automatisch erkannt und zur weiteren Verarbeitung in datenverarbeitende Einrichtungen weitergegeben werden. So gibt es insbesondere Einrichtungen, die Ziffern aufnehmen und in Rechner eingeben, so daß eine Tastatur zur Eingabe vermieden werden kann. Derartige Einrichtungen sind bisher noch nicht im großen Umfange eingeführt, weil von ihnen gefordert wird, daß sie Worte gesprochen von vielen verschiedenen Personen erkennen, wodurch die Erkennungssicherheit nur mit relativ großem Aufwand zu erzielen ist.

Weiterhin sind Einrichtungen unter dem Stichwort "voice-print" bekannt geworden. Diese Einrichtungen gestatten es, eine Person, die eine begrenzte Anzahl Worte spricht, zu identifizieren, und unter vielen anderen Personen eindeutig zu unterscheiden.

Das im folgenden beschriebene Verfahren stellt eine Ergänzung zu oder einen Ersatz für die PIN durch ein gesprochenes Wort dar. Es vermeidet gleichzeitig die Schwierigkeiten der beiden oben genannten Ausgangsverfahren.

Die in Fig. 5 dargestellte Dokumentensicherungs-Einrichtung hat mit der in Fig. 3 dargestellten Einrichtung große Ähnlichkeit. Zum Unterschied gegenüber dem anhand der Fig. 3 beschriebenen Verfahren wird aber hier vorausgesetzt, daß das in das Bandgerät 21 eingelegte Band nicht nur in digitaler Form die Personalisierungsdaten enthält, sondern darüberhinaus ein während der dezentralen Herstellung des Bandes vom zukünftigen Inhaber des Ausweisdokumentes gesprochenes Codewort.

Die meisten in der Dokumentensicherungs-Einrichtung nach Fig. 5 sich abspielenden Vorgänge entsprechen denen, die anhand der Fig. 3 erklärt wurden. Es ist lediglich auf dem Weg von dem Bandgerät 21 zum Algorithmusrechner 5 ein zusätzliches Sprachverschlüsselungsgerät 50 angeordnet, das

die digitale Information vom Band ungehindert in den Algorithmusrechner 5 einfließen läßt, die im Band enthaltene Sprachinformation, also das gesprochene Codewort, jedoch in eine digitale Information umwandelt, die dann, wie bereits beschrieben, verschlüsselt und verarbeitet wird.

Das Sprachverschlüsselungsgerät 50 kann in bekannter Weise aufgebaut werden. Es kann aus der Technik der Worterkennungsgeräte und der der "voice-print"-Technik eine Reihe von Methoden und Elementen entnehmen, ohne jedoch den besonderen Schwierigkeiten dieser beiden Techniken gerecht werden zu müssen.

Auf diese Weise wandelt das Sprachverschlüsselungsgerät nicht nur die klanglichen Eigenschaften eines bestimmten Wortes, sondern zusätzlich auch die klanglichen Besonderheiten der Stimme des rechtmäßigen Inhabers des Dokumentes in digitale Form um, die dann verschlüsselt wird.

In Fig. 6 ist das der Fig. 4 entsprechende Dokumentenkontrollgerät dargestellt. Es unterscheidet sich von diesem nur dadurch, daß die Eingabevorrichtung 28 durch ein Mikrofon 51 und das bereits beschriebene Sprachverschlüsselungsgerät 50 ersetzt ist. Bei der Benutzung hat der Teilnehmer das Codewort in das Mikrofon 51 zu sprechen. Diese analoge

Information wird vom Sprachverschlüsselungsgerät 50 digitalisiert und genauso wie die PIN in dem anhand der Fig. 4 beschriebenen System mit der entsprechend entschlüsselten Information des Dokumentes verglichen.

Es wurde oben bereits darauf hingewiesen, daß bildliche Darstellungen, wie Fotos, Unterschriften oder Fingerabdrücke, in das Verfahren einbezogen werden können, um sie gegen Veränderungen abzusichern, die bei der für diese bildlichen Darstellungen erforderlichen visuellen Kontrolle übersehen werden könnten. Für eine derartige Absicherung ist eine eindeutige Digitalisierung der bildlichen Darstellung notwendig, da gerade gute Verschlüsselungsverfahren bekannterweise bei kleinen Veränderungen am Klartext K zu großen Änderungen an der chiffrierten Information C führen, die eine Entschlüsselung später unmöglich machen. Für Unterschriften und Fingerabdrücke liegen bereits Abtast- und Digitalisierungsverfahren vor, die diesen Ansprüchen genügen.

Von besonderer Bedeutung für die visuelle Kontrolle z.B. von Paßkarten ist das Foto des rechtmäßigen Inhabers. Das im folgenden beschriebene Verfahren dient ebenso wie ähnliche Verfahren zur Abtastung der Unterschrift oder des Fingerabdrucks in der Hauptsache dazu, die Unversehrtheit dieser für die visuelle Kontrolle erforderlichen Ele-

mente des Dokumentes durch eine automatische Kontrolle abzusichern. Ein für die Digitalisierung derartiger Fotos besonders geeignetes Verfahren sei anhand der schematischen Darstellung nach Fig. 7 beschrieben. Die Paßkarte 30 trägt ein Foto 31, von dem nur vorausgesetzt wird, daß es eine bestimmte Minimalgröße in beiden Ausdehnungen nicht unterschreitet. Auf dieses Foto wird ein gedachtes Rasterfeld 32 gelegt, das eine vorzugsweise quadratische Rasterteilung aufweist. Dieses gedachte Rasterfeld 32 beschreibt die Abtastfolge eines Abtastgerätes, das mit einem Abtaststrahl arbeitet, dessen Bewegung mit aus der Abtasttechnik bekannten Einrichtungen bewirkt wird.

Ebenfalls nach bekannten Methoden und mit bekannten Einrichtungen wird das gedachte Abtastfeld 32 vor der Abtastung so verschoben, daß z.B. die linke obere Ecke und die linke und die obere Kante des Abtastfeldes mit der linken oberen Ecke und den entsprechenden Kanten des Fotos 31 übereinstimmen.

In Fig. 8 ist in schematischer Darstellung die Verarbeitung des abgetasteten Signals, also der Helligkeitswerte der Einzelquadrate des Abtastrasters 32, dargestellt. Hierbei wird angenommen, daß für die Helligkeitsmessung der nacheinander beleuchteten Rasterelemente eine einzige

lichtempfindliche Zelle vorgesehen ist, aus der die Helligkeitswerte der einzelnen Rasterelemente in serieller Form abgegeben werden.

Das im folgenden beschriebene Verfahren läßt sich aber auch auf andere Abtastanordnungen - beispielsweise lineare oder flächige Diodenarrays - übertragen.

Die in Fig. 8 dargestellte Einrichtung arbeitet folgendermaßen:
Die von einem Bildrasterabtastgerät in Form eines Lichtempfängers 33 abgegebene, mit der Helligkeit der Rasterpunkte des Rasterfeldes 32 schwankenden Impulse werden einem regelbaren Verstärker 34 und anschließend einer Selektionsstufe 35 zugeführt, die entscheidet, ob der Impuls größer oder kleiner als ein fest eingestellter Wert ist. Die Impulse, die den fest eingestellten Wert überschreiten, werden in einem Zähler 36 gezählt. Impulse, die den Wert unterschreiten, werden in einem Zähler 37 gezählt. Jeweils nach vollständiger Abtastung des gesamten Rasters werden die Zählerstände der Zähler 36 und 37 in einen Vergleicher 38 miteinander verglichen. Falls sie nicht ein vorgeschriebenes Verhältnis (z.B. 1:1) besitzen, wird über eine Regelleitung 39 der regelbare Verstärker 34 nachgestellt.

Diese Prozedur wird solange wiederholt, bis das vorgegebene Verhältnis der Zählerstände in den Zählern 36 und 37 erreicht ist. Damit ist gesichert, daß der durch das Rasterfeld 32 überdeckte Teil des Fotos 31 in ein Bit-Muster verwandelt ist, das einen vorgeschriebenen Anteil an "hellen" Rasterpunkten und entsprechend einen vorgeschriebenen Anteil an "dunklen" Rasterpunkten enthält. Dieses Bit-Muster wird als die dem Foto zugeordnete Information abgespeichert und dem beschriebenen Verschlüsselungsverfahren unterworfen.

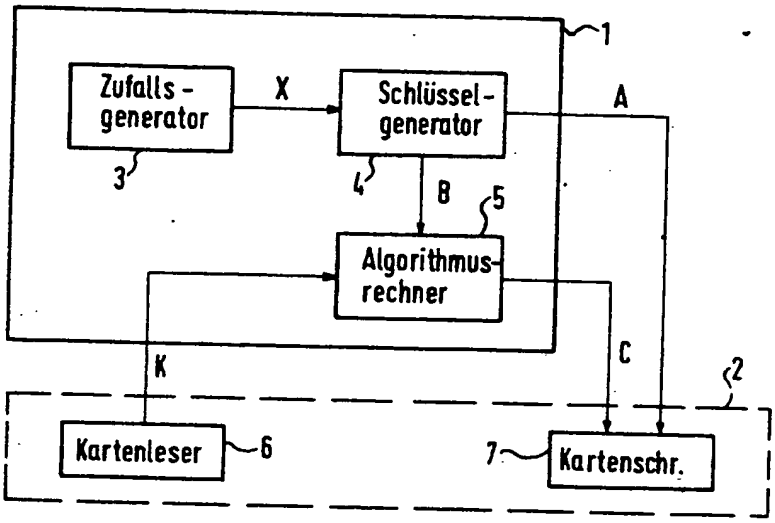
In Fig. 8 sind alle für den Gleichlauf von Abtastung und Zählung notwendigen Elemente nicht dargestellt worden, da sie zum bekannten Stand der Technik gehören.

Nummer: 28 26 469
Int. Cl.²: G 07 C 9/00
Anmeldetag: 16. Juni 1978
Offenlegungstag: 20. Dezember 1979



2826469

Fig. 1



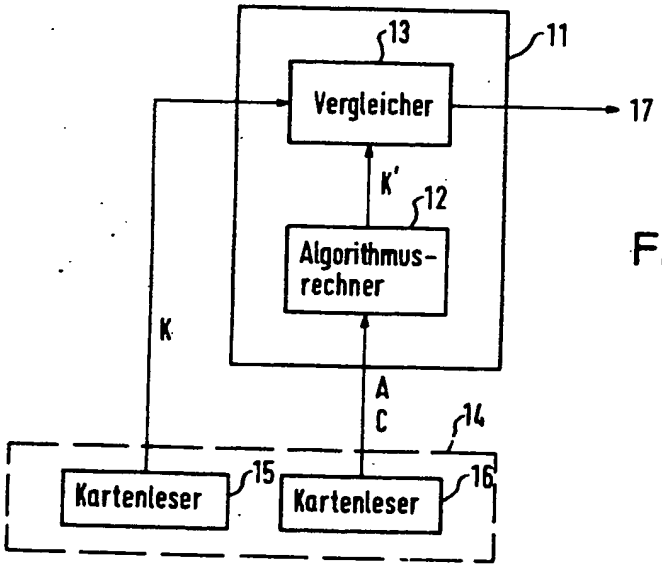
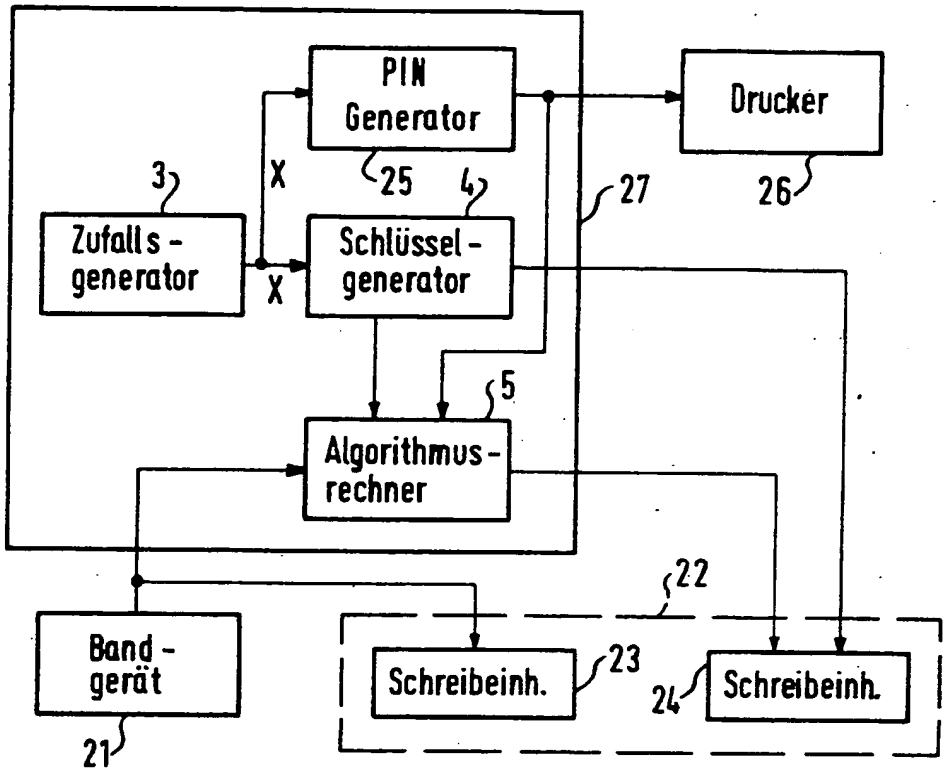




Fig. 2

Fig. 3


PIN Generator
Drucker
25
26
3
X
4
27
Zufalls - generator
X
Schlüssel - generator
5
Algorithmus - rechner
22
Band - gerät
Schreibeinh.
23
24
Schreibeinh.
21

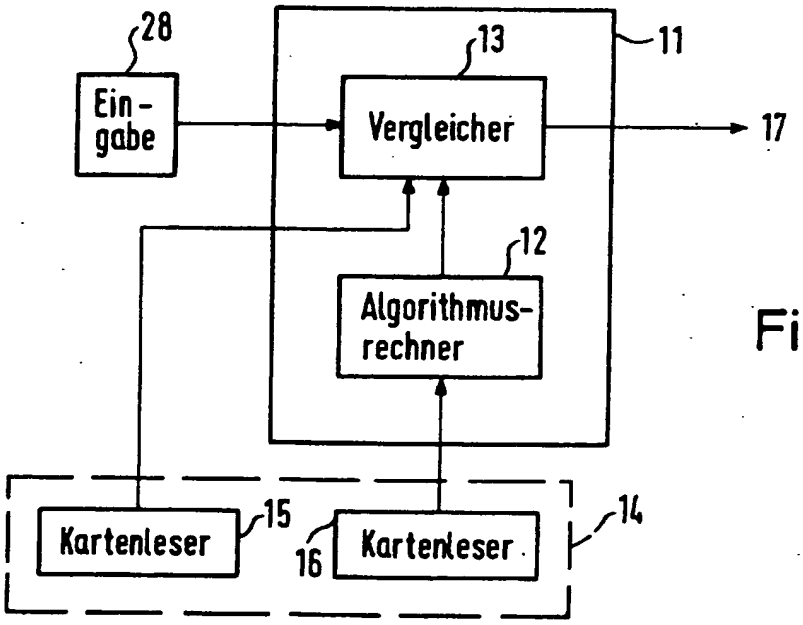

28
13
11
Ein - gabe
Vergleicher
17
12
Algorithmus - rechner
Kartenleser
15
16
Kartenleser
14

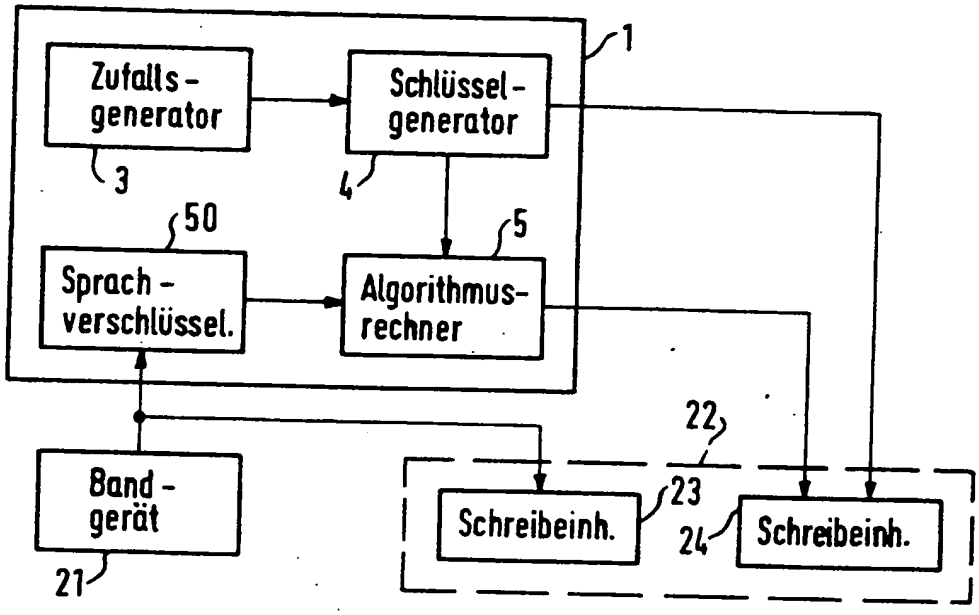
Fig. 4

10-08-78





Fig. 5



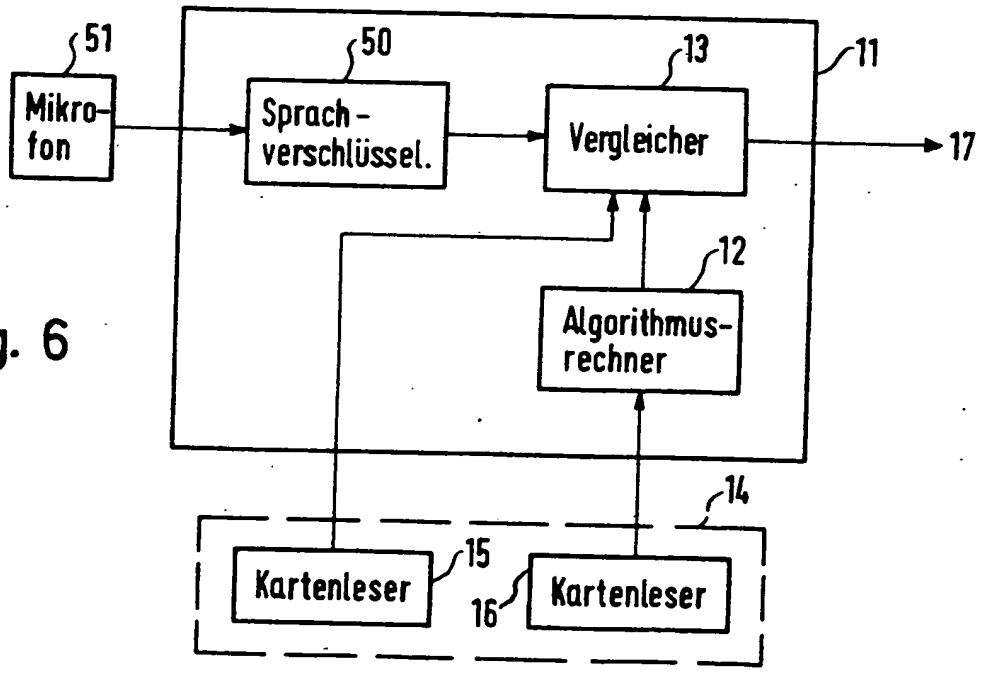
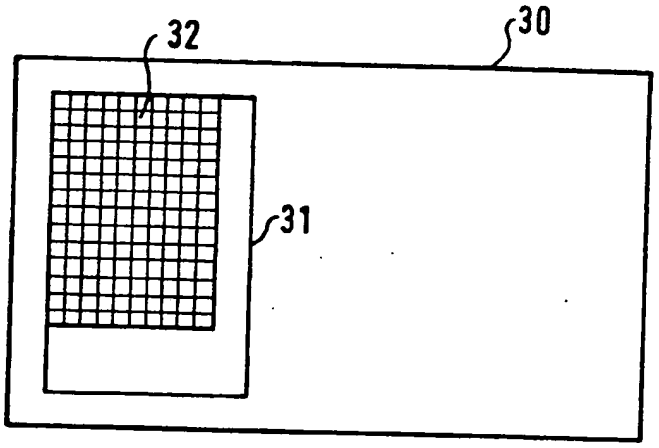




Fig. 6

Fig. 7



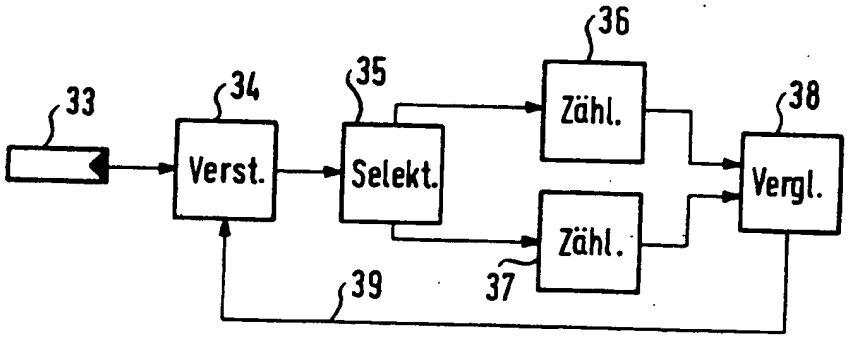




Fig. 8